

## TECHNOLOGY USE AND PRIVACY GUIDELINES

Please read this document carefully. When signed by you, it becomes an agreement between you and the District. Your signature indicates that you have read understand and agree to abide by the conditions and guidelines established herein.

SUSD provides various Technology Resources to authorized employees to assist them in performing their job duties. Each employee has a responsibility to use the District's Technology Resources in a manner that is respectful of other employees, and consistent with the educational goals and objectives of the District. Each employee is responsible to report any misuse of the network to the Director of Information Technology. Each employee is further responsible for the supervision of students using the District's Technology Resources. Failure to follow the District's policies regarding Technology Resources may lead to disciplinary measures up to and including termination. Illegal uses of District Technology may result in referral to law enforcement authorities. SUSD Acknowledges that this policy is intended for activity generated by school employees. It is understood that this policy cannot address actions or activities that may be initiated outside of the District.

### ***Technology Resources Defined***

"Technology Resources" consist of all electronic devices, software, and means of electronic communication including, but not limited to: personal computers and workstations; lap-top computers; mini and mainframe computers; computer hardware; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including software that grants access to external services, such as the Internet, or the SUSD Intranet; electronic mail; telephones; cellular phones; pagers; PDAs; and voicemail systems or other technology related resources.

### ***Authorization***

Access to the District's Technology Resources is within the sole discretion of the District. Generally, employees are given access to the District's various technologies based upon their job functions. The use of the District's Technology Resources may be revoked by the District, at any time for any reason.

### ***Use***

The District's Technology Resources are to be used by employees for the purpose of conducting District business. Incidental personal use of District computers is permitted as long as the use does not result in any additional cost to the District and does not interfere with the employee's job duties and performance, with system operations, or with any other system user. "Incidental personal use" is defined as incidental, occasional and reasonable use by an individual employee for personal communications. Such personal use must comply with this policy and all other applicable policies, procedures and rules.

### ***Improper Use***

#### ***1. Harassing, Discriminatory and Defamatory Use***

As set forth more fully in the District's personnel policies, the District will not tolerate discrimination or harassment against any individual based on his or her race, religion, color, national origin, gender, sexual orientation, gender identity, age, disability or veteran status – even if the law does not prohibit the conduct. Under no circumstances may employees or students use the District's Technology Resources to transmit, receive, or store any information that is discriminatory, harassing, defamatory, or verbally abusive in any way (e.g., sexually-explicit or racial messages, jokes, or cartoons).

#### ***2. Inappropriate Communications With Students or Minor***

The District will not tolerate any inappropriate communication with any student or minor. Any such use will result in disciplinary measures up to and including termination.

#### ***3. Copyright Infringement***

Employees may not use the District's Technology Resources to copy, retrieve, forward or send copyrighted materials unless the employee has the author's permission or is accessing a single copy only for the employee's reference.

#### ***4. Unlawful Activity***

Employees may not use the District's Technology Resources to engage in any activity constituting or

promoting a criminal offense, or potentially giving rise to civil liability, or otherwise violating any law, regulation, or District policy.

**5. *Conflict of Interest.***

Employees may not use any of the District's Technology Resources to further any business activity in which the District has no interest. Employees may not use any of the District's Technology Resources in a manner that results in unauthorized billing or direct costs to the District or that is otherwise contrary to the best interests of the District.

**6. *Confidential and Proprietary Information.***

Employees may not use the District's Technology Resources in any manner that discloses confidential or proprietary information of the District to third parties.

**7. *Use of District technology resources to influence the outcome of elections.***

Employees may not use the District's Technology Resources for the purpose of influencing the outcomes of elections, or to advocate support for or opposition to pending or proposed legislation by initiating such activity through District Technology Resources.

**8. *Other Improper Uses.***

Employees may not download material from the Internet or load software or applications that have not been approved for installation on a District computer or network without advanced written permission from the Director of Informational Technology or his/her designee. Employees may not use District Technology Resources to solicit funds; distribute chain letters; sell merchandise or services; collect signatures; or conduct membership drives.

***District Access to Technology Resources***

All messages sent and received, including personal messages, and all data and information stored on the District's electronic-mail system, voicemail system, or computer systems are District property regardless of the content. As such, the District reserves the right to access all of its Technology Resources including its computers, voicemail, and electronic-mail systems, at any time, in its sole discretion.

***Privacy***

Employees should understand that they have no reasonable expectation of privacy with respect to any messages or information created or maintained on the District's Technology Resources, including personal information or messages. The District may, at its discretion, inspect all files or messages on its Technology Resources at any time for any reason. The District may also monitor its Technology Resources at any time in order to determine compliance with its policies, for the purposes of legal proceedings, to investigate misconduct, to locate information, or for any other purpose consistent with its educational goals and objectives.

***Passwords***

Certain of the District's Technology Resources can be accessed only by entering a password. Passwords are intended to prevent unauthorized access to information. Passwords do not confer any right of privacy upon any employee of the District. Thus, even though employees may maintain passwords for accessing Technology Resources, employees must not expect that any information maintained on Technology Resources, including electronic-mail and voicemail messages, are private. Employees are expected to maintain their passwords as confidential. Employees must not share passwords and must not access coworkers' systems without express authorization. Upon request from the Director of Information Technology or designee, employees must disclose their passwords to facilitate access by the District.

***Deleted Information***

The best way to guarantee the privacy of personal information is not to store or transmit it on the District's Technology Resources. Deleting or erasing information, documents, or messages maintained on the District's Technology Resources is, in most cases, ineffective. All employees should understand that any information kept on the District's Technology Resources may be electronically recalled or recreated even after it has been "deleted" or "erased" by an employee. Because the District periodically backs-up all files and messages, and because of the way in which computers re-use file storage space, files and messages may exist that are thought to have been deleted or erased. Therefore, employees who delete or erase information or messages should not assume that such information and/or messages are confidential.

***Internet and Electronic Mail Policy***

The District expects that when employees use the Internet or electronic mail during work hours, non-work hours, while on the District's premises, or remotely through the use of the District's computer equipment, they will do so

in a responsible manner.

Improper use of the Internet and electronic mail includes, but is not limited to the following:

- Use that is illegal, contrary to the District's best interests, or violates or conflicts with the District's policies, including, but not limited to, the District's policies against discrimination or harassment.
- Use that discloses or leads to the disclosure of confidential or proprietary information about the District.
- Use of electronic mail, chat rooms or other Internet devices that is defamatory or offensive in any way, including, but not limited to, racially or sexually explicit messages, jokes or cartoons.
- Use of Internet sites that may damage or interfere with the District's computer network, including use that generates the delivery of "junk" electronic mail.
- Use that violates copyright laws.
- Personal use, and/or use that is not work-related; except that use defined as "incidental personal use".
- Any communications that are in violation of generally accepted rules of network etiquette and/or professional conduct.

Illegal uses of District Technology may/will also result in referral to law enforcement authorities. Improper use of the Internet or electronic mail may lead to discipline up to and including termination.

Employees have no right of privacy, nor any expectation of privacy, with respect to any aspect of their use of the Internet or electronic mail while on the District's premises, or when accessing the Internet or using electronic mail remotely. The District reserves the right to, at any time, and without limitation, monitor employee use of the Internet, including monitoring Internet sites visited, the number of times those sites are visited and the time connected to each site. The District reserves the right to limit such access by any lawful means available to it, including revoking access altogether.

#### ***Confidentiality***

Employees should use caution when sending confidential information over the Internet. Employees also should try to verify electronic mail addresses before transmitting any messages.

#### ***Software Use***

All software in use on the District's Technology Resources is officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No employee may load any software on the District's computers, by means of transmission, unless authorized in writing in advance by the Director of Information Technology. Authorization for loading software onto the District's computers should not be given until the software to be loaded has been thoroughly scanned for viruses.

#### ***Security***

The District has installed a variety of programs and devices to ensure the safety and security of the District's Technology Resources. Any employee found tampering and/or disabling any of the District's security devices will be subject to discipline up to and including termination.

The District is not liable for employee submission of credit card or other sensitive data over the internet.

**I have read and understand the SUSD Technology Use and Privacy Policy and agree to abide by all of the provisions of the Policy.**

**Print Name:** \_\_\_\_\_

**Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_